Retina Based Marine Predators Optimization For Secured Key Generation

[1]N.Malathy* , [2]A.Vidhya and [3]R.Tamilroja

[1]Asisstant Professor (senior Grade) Department of Information Technology Mepco Schlenk Engineering College, Sivakasi.

[2]Asisstant Professor Department of Computer Science and Engineering Jeppiaar Engineering College, Chennai.

[3]Asisstant Professor Department of Computer Science and Engineering jeppiaar SRR Engineering College, Chennai.

Abstract

The use of retrieved features from human anatomical (physiological) attributes like a fingerprint, retina, etc., or behavioral attributes like a autograph is referred to as biometric-based keys creation. As the biometric using retina has intrinsic strength, it can generate arbitrary keys with a more level of security than the rest of the biometric features. In this work, a system for cryptographic applications that generate safe, strong, and exclusive arbitrary keys depends on retina properties. The features of retina are retrieved using the Marine Predators algorithm (MPA) which has been shown to produce promising results in studies by utilizing common retina databases. The proposed system has also used the chaotic map to offers premium arbitrary, volatile, and non-producible keys. Also to check the assurance and randomness of the binary key generation the NIST statistical analysis is performed to show the effectiveness of the proposed work.

Keywords: Arbitrary keys, Chaotic map, Marine Predators Algorithm (MPA), Retina, Secured key generation.

Introduction

To design the cryptographic system two major phases are needed; the cryptographic key and the cryptographic algorithm. The cryptographic algorithm gets strengthened based on the security level of the generated keys. Most of the security algorithms consist of arbitrary, safe, and difficult to remember with large keys. There exist two classes in the generation of key: Pseudo-Random Number Generation (PRNG) and True-Random Number Generation (TRNG). In the PRNG phase, the keys are generated randomly based on the initial security condition but the major security condition gets violated in this method. This leads to the attacker intruding on the system easily whereas in TRNG the keys are produced depending on unpredictable physical resources.

There exist lots of traits including fingerprints, retina, and face biometrics but they are not similar to either individual. Hence these traits can be used for producing secured keys for secured domains. The major phase involved in these biometric-based key generations is feature extraction. The best one among the extracted feature is selected and then integrates with a cryptographic algorithm. The human retina-imposed cryptographic system has certain priorities compared to another biometric-based system as the retina has a certain unique vascular pattern and also it is implanted in the depth of the human body which is unaltered. And also the retina pattern does not change even with the aging factor.

In the recent era, nature-inspired optimization algorithms have attained familiarity to solve a complex real-world problem in which a solution is not feasible. Compared with other metaheuristics algorithms the marine predator's algorithm has many benefits like simple, better search, and easy implementation. There exist more swarm intelligence algorithms in different applications. In this work, the behavior of marine predators is applied to extract the optimal features from the retinal image. This optimal feature is utilized as the major source and it is called a biometric-based key generation (BBKG) together with the chaotic map to produce the encryption keys. The paper is arranged as follows: The necessary information of the interrelated system is reviewed in section two; The marine predators algorithm is discussed in section three. The proposed system is illustrated in section four and the experimental results are explained in section five.

Related works

The human biometric behavior characterize the major source of entropy to produce arbitrary numbers close to the TRNG. But all the traits cannot be considered for key generation, a certain comprehensive exam is needed to check whether the trait is suitable or not [8]. Recently many researchers worked in the key generation system based on biometrics. Some of the applications are combined with a chaotic map to acquire not predictable arbitrary keys for secured applications and the produced keys are verified with statistical analysis test, NIST.

The key generation system based on iris was proposed by the author in [1].In this method, the iris edge is represented as a binary image based on the feature extracted by applying a canny edge detector and chaotic map to come out of a similar pattern collected from the same person. In [2] the authors applied three-level Haar wavelet transform (HWT) on the iris picture and the features are represented as coefficients acquired from middle-frequency sub-bands. And then these coefficients are encoded as binary values based on their negative and positive values. The keys extracted from the above method find more robustness compared to others. In [3] the authors proposed a key generation system based on brain waves in which the human's Electroencephalogram (EEG) signal is considered for producing a unique key. In this approach, the keys are generated based on Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). The authors in [4] indicate that the EEG signal cannot be directly used as a major resource for producing keys. It has to be transmitted into a suitable format as this represents the major challenging task compared to other traits.

A fingerprint-based key generation system was proposed in [5]. This system works in different steps. In the first step, the fingerprint is split into different blocks. Next in the second step for every blocks the delta, core, and minutiae points are extracted. Second, all straight lines are computed from one minutiae point in a reference block to all minutiae points in all nearby blocks. Also, the straight lines between the minutiae points within the reference block are evaluated. Last, delta and core points are used to calculate the angle and length of each straight line. Fourth, every straight line's attribute is transformed to a binary form, and then an XOR operation is done among each binary bit of angle and length. This scheme may generate various s keysecured depending on a variety of criteria such as the number of blocks and the size of the block. The biggest drawback of this technique is the inability to keep certain attributes hidden.

In [6] the authors developed a key generation system depending on retina in which the key creation process is divided into two stages: first, preprocessing of retina image, and second, segmentation of image using the grayscale morphology method. Third, the entropy approach is used to extract features, fourth, an adaptive canny edge detection algorithm is used to estimate the retina center, and fifth, linear interpolation is used to connect the retina center points. Eventually, the coordinates of these additional points are located in the chaotic matrix's key values. Randomness, unpredictability, and non-repeatability are provided in this approach by using a chaotic map with retinal properties to generate cryptographic keys.

Even though many of the methods listed above passed the majority of the NIST tests, they neglected the resilience of keys that may be gained by retrieving the strongest and most optimal characteristics from the biometric attributes used. As a result, to meet this important need; First, the proposed retina-based key generation system employs the Low-frequency sub-band of the HWT of the retina image because it contains the majority of the image's energy, making it the best location for extracting retina features; second, the MPA has been used to extract the best features from the LL sub-band of the retina image.

Materials and Methods:

Marine Predators Algorithm

A new meta-heuristic algorithm is known as Marine Predators Algorithm (MPA)[7] has been developed to tackle the continuous optimization problems. It consists of two strategies when attacking that is Brownian and Levy. To begin the process the first step needed to implement is the initialization process. The second step is to create the Elite and Prey matrix construction. Then the optimization process consists of three categories the first step in the optimization process is the Brownian movement in which the exploration phase is executed the second phase consists of two categories in which the population is divided into two, the first half of the population means that the end of exploration phase and the second half of the population consists of the start of exploitation phase. The third stage is the Levy flight phase in which the predators relative to their environment. The detailed explanation and the equation used are as follows:

Initialization:

MPA starts with spreading their solutions within the search space of the problem using the following formula:

$$\vec{X} = \vec{X}_L + rand * (\vec{X}_U - \vec{X}_L) \tag{1}$$

$\overrightarrow{X_L}$ and $\overrightarrow{X_U}$ are Maximum and Minimum of the boundary of the Search space.

Elite and Prey Matrix:

The Elite and Prey Matrix for the MPA algorithm can be represented as:

$$E = \begin{bmatrix} X^{|}_{1,1} X^{|}_{1,2} \ldots\ldots\ldots X^{|}_{1,d} \\ X^{|}_{2,1} X^{|}_{2,2} \ldots\ldots\ldots X^{|}_{2,d} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X^{|}_{n,1} X^{|}_{n,2} \ldots\ldots\ldots X^{|}_{n.d} \end{bmatrix}$$

$$P_Y = \begin{bmatrix} X_{1,1} X_{1,2} \ldots\ldots\ldots X_{1,d} \\ X_{2,1} X_{2,2} \ldots\ldots\ldots X_{2,d} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n,1} X_{n,2} \ldots\ldots\ldots X_{n,d} \end{bmatrix} \tag{2}$$

Optimization Process:

Brownian Phase:

In this phase, the predators try to move faster until finding their prey as the nature, while

$$t < 1/3 * t_{\max}$$
$$\vec{S}_i = \vec{R}_B \otimes (\vec{E}_i - \vec{R}_B \otimes p\vec{y}_i)$$
$$p\vec{y}_i = p\vec{y}_i + p * \vec{R} \otimes \vec{S}_i \tag{3}$$

Where $\vec{S_i}$ - refers to the current Step Size of the ith predator

$\overrightarrow{R_B}$ -Vector Containing Numerical Values generated randomly using Gaussian

$\otimes$-Element-wise Multiplication

t- Current iteration

$t_{\max}$ - Maximum iteration

Levy Phase:

In this phase, the balance between exploration and exploitation can be calculated using the

$$\begin{aligned}
&t < 1/3 * t_{\max} < t < 2/3 * t_{\max} \\
&\vec{S}_i = \vec{R}_L \otimes (\vec{E}_i - \vec{R}_L \otimes p\vec{y}_i) \\
&p\vec{y}_i = p\vec{y}_i + p * \vec{R} \otimes \vec{S}_i \\
&\vec{S}_i = \vec{R}_B \otimes (\vec{R}_B \otimes \vec{E}_i - \vec{P}_i) \\
&p\vec{y}_i = \vec{E}_i + P * C.F \otimes \vec{S}_i
\end{aligned} \tag{4}$$

$\overrightarrow{R_L}$ -Vector Containing Numerical Values generated randomly using Levy Flight

Levy Flight:

In this phase, the prey will move faster compared to predator as the nature while,

$$\begin{aligned}
&it < 2/3 * \max\_iter \\
&\vec{S}_i = \vec{R}_L \otimes (\vec{E}_i \otimes \vec{R}_L - p\vec{y}_i) \\
&p\vec{y}_i = \vec{E}_i + p * CF \otimes \vec{S}_i
\end{aligned} \tag{5}$$

Where $\overrightarrow{S_i}$ - refers to the current Step Size of the ith predator

$\overrightarrow{R_L}$ -Vector Containing Numerical Values generated randomly using Levy Flight

$\overrightarrow{E_i}$ -Energy Consumption

Fish Aggregating Devices:

In this, the prey will Search for the corresponding within the Surrounding environment

$$P\vec{y}_i = \begin{cases} P\vec{y}_i + CF\left[R \otimes \vec{X}_U - \vec{X}_L\right] \otimes \vec{U} \\ P\vec{y}_i + \left[FADS(1-r) + r\right](P\vec{y}_{r1} - P\vec{y}_{r2}) \end{cases} \tag{6}$$

$\overrightarrow{Py_i}$ -Vector value for prey

$\overrightarrow{X_L}$ and $\overrightarrow{X_U}$ are Maximum and Minimum of the boundary of the Search Space.

$\overrightarrow{Py_{r1}}$ and $\overrightarrow{Py_{r2}}$ are the two predators selected randomly?

$\vec{U}$ - vector which includes 0 and 1 values.

Proposed Method

Retina-based Key Generation System

The proposed system consists of four main phases: image acquisition and preprocessing, isolation of the preprocessed retina image into four sections using the Discrete Wavelet Haar Transform

(DWHT), retrieval of the optimal features using the GSO algorithm, and finally unification of the optimal features with the Chaotic map to generate the arbitrary cryptographic key. The suggested retina-based key generation system is depicted in Figure 1 is a block diagram.

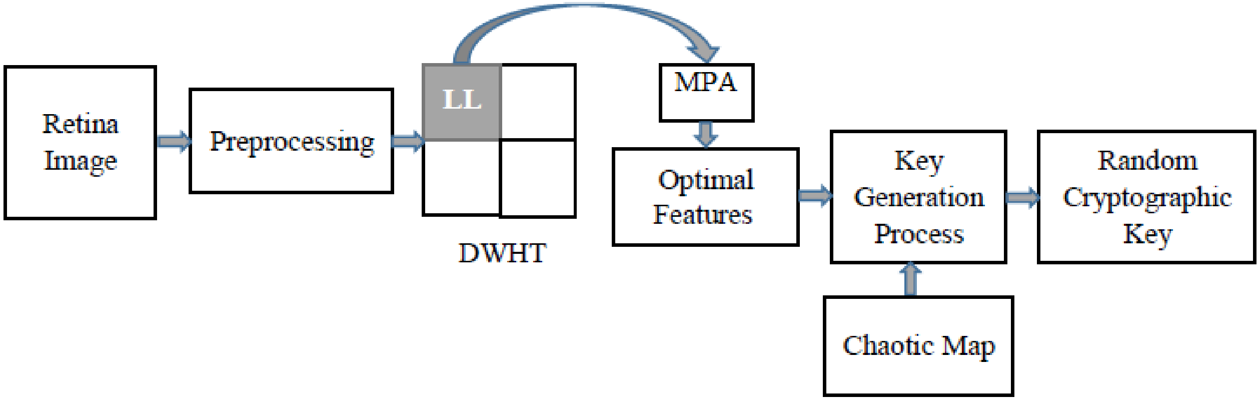


Figure 1 proposed system

Acquisition and Preprocessing of Retina Images

The term "retina image acquisition" refers to the process of acquiring a retina image with any retina camera now available on the market. The DRIONS-DB (Digital Retinal Images for Optic Nerve Segmentation Database), a publically available database, was employed in this study. The supplied retina image must then be preprocessed after that. Several processes are included in the preparation stage:

The first pre-processing step is to transform RGB color images into Grayscales to reduce the number of colors. For each (k j) pixel, the RGB components are separated from the 24-bit color value, and an 8-bit grayscale value is generated. The average weight for the RGB value is calculated during the conversion process.

$$Grayscale(k,j)=((0.3*R)+(0.59*G)+(0.11*B)) \qquad (7)$$

The second phase in the pre-processing process is to use an adaptive Histogram Equalization algorithm to adjust the distance between every two consecutive grey levels in the histogram, preventing severe grey pixel mergers and exceptionally bright local spots in the image. This procedure is as follows: first, save the original grey levels image as f_i, where i=1,..., m-1, and then use the ratio $\sum_{i=0}^{k-1} H_p \ \sum_{i=k+1}^{n-1} H_p$ to get the location j of the mapped grey level g_i. Then, compare i with j, and if j is greater than i map forward; if j is less then i map backward.

$$= (n-1) \frac{\sum_{i=0}^{k-1} H_p}{\sum_{i=0}^{k-1} H_p + \sum_{i=k+1}^{n-1} H_p} \qquad (8)$$

Where n is the number of grey levels in the input images, $\sum_{i=0}^{k-1} H_p$ is equal to 1, $H_p=q_p/T$, q_p is the number of image pixels of the pth grey level, and T is the total number of pixels in the image. The gray level with a small number of pixels can then be phagocytosed via the gray level with a large number of neighbor pixels during the mapping process. In grey mapping, an adaptive parameter ∂

based on information entropy is included to prevent the phenomenon of information loss. The mapping relationship is as follows:

$$q_p=\log(q_p + 1) \quad (9)$$

$$j=(n-1) \frac{\sum_{i=0}^{k-1} H_p}{\sum_{i=0}^{k-1} H_p + \sum_{i=k+1}^{n-1} H_p}, \partial \in (0,+\infty) \quad (10)$$

The median filter is applied as the third pre-processing phase. This method is frequently used to eliminate noise. Reducing noise is a common pre-processing phase used to enhance the outcome of subsequent processing The Canny edge detection filter is used as the final pre-processing step to spot and identify edges of vessel..

Discrete Wavelet Haar Transform (DWHT)

The 1-level DWHT decomposes the pre-processed image into four sub-bands by first executing the row and next column, resulting in the four sub-bands termed (LL, LH, HL, HH). The functional sub-band is represented by LL, and it contains the entire procedure that will be applied to the figure.

Extraction of the Best Features applying MPA

The basic goal of MPA is to find the best features in the chosen sub-band "LL." The MPA is applied as follows: First, initialize the Elite and prey matrix. Then to find the optimal feature Brownian and levy flight movement is applied by using equations (3) to (6) until the optimum feature is selected.

Process of Key generation:

The amount of ideal pixels retrieved from the retina diagrams determines the length of the generated cryptographic keys; in this work, the size of the obtained keys is 128 bits, hence the amount of effectively retrieved pixels is 16. In this phase, the optimum retinal features (the extracted sixteen pixels) from the preceding phase are XORed with arbitrary bits produced from a kind of Chaotic map to construct a 128-bit cryptographic key. The Tent map, a one-dimensional Chaotic system, is employed in this paper, and its equation is as follows:

$$Y_{n+1} = \begin{cases} \frac{Y_n}{\eta}, 0 \le Y_n \le \eta \\ (1-Y_n)/\eta, \eta \le Y_n \le 1 \end{cases} \text{ where } \eta \in (0,1).\ \eta \neq 0\cdot 5, here, \eta = 0.62 \quad (11)$$

Experimental Findings:

The suggested scheme is experienced and assessed on the DRIONS-DB database, which contains 110 retina bitmap images with a resolution of 24 bits per pixel and a size of (565x584). The produced binary bits key was checked for randomness using the NIST Test Suite, which contains 10 statistical tests. Figure 2 shows four samples of retina images from the dataset in question. There are two key stages previous to the procedure of remove the ideal features: the primary is the pre-processing phase, which focuses on detecting blood vessels with high resolution, and the next is take out the LL sub-bund following implementation of the 1-level DWHT. Figures 3, 4, 5, and 6 illustrate the retinal diagrams obtained after completing the above steps.

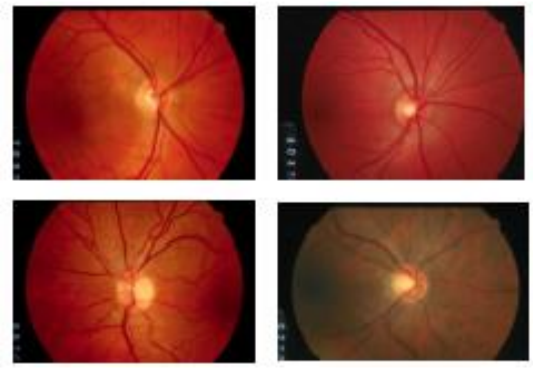


Figure 2. Sample images of Retina from DIRONS-DB.

The paths of glowworms from their initial sites to their ultimate locations (optimal solutions) for the retina image samples are depicted in Figure 7. Figure 8 shows the produced 128-bit cryptographic key for each retina picture sample. Table 2 also includes the NIST Test Suite results for the created cryptographic keys, which showed that they passed all of the NIST tests.

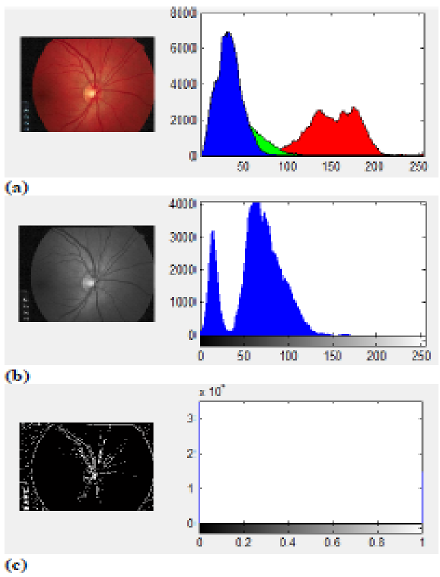


Figure 3. (a) sample retina image, (b) grayscale image, (c) after preprocessing and decomposition

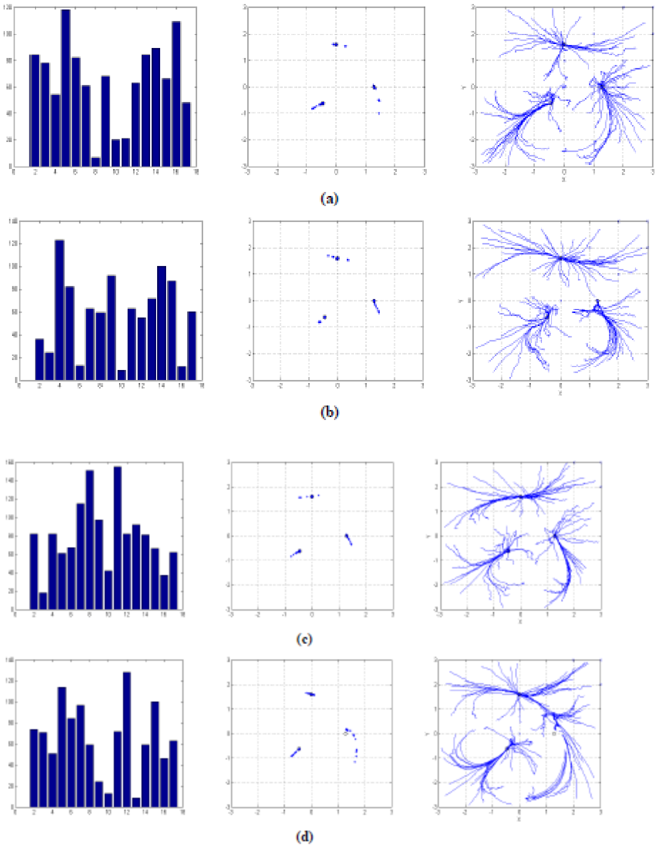
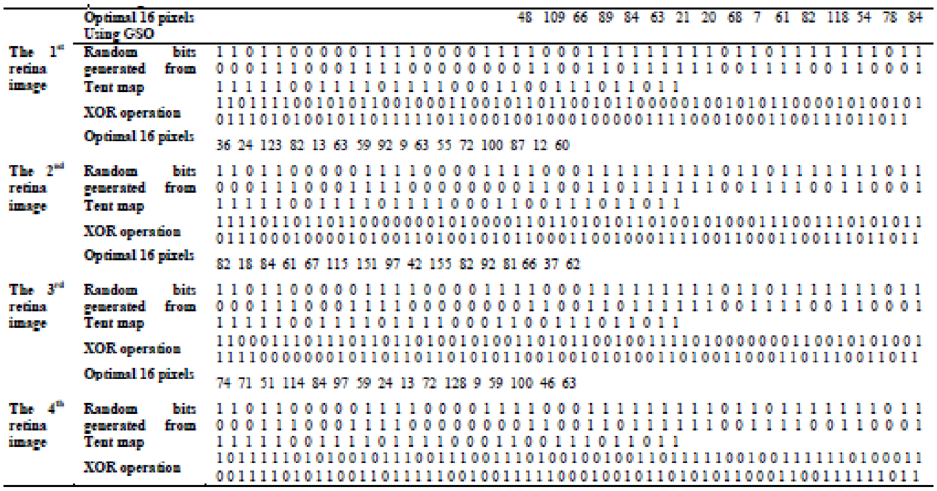


Figure 7. a) to (d), depicts the trajectories of predators starting with preliminary positions till accomplishing the final position, the next diagram depicts the best position, and the third diagram characterize the values of 16 optimum pixels, for the four samples of retinal diagram



	Optimal 16 pixels Using GSO	48 109 66 89 84 63 21 20 68 7 61 82 118 54 78 84

The 1st retina image	Random bits generated from Tent map	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 1 0 1 1
		0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1
		1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1

	XOR operation	110111100101011001000110010110110010110000010010101100001010 0101 0111010100101101111110110001001000100000111100010001100111011011
	Optimal 16 pixels	36 24 123 82 13 63 59 92 9 63 55 72 100 87 12 60

The 2nd retina image	Random bits generated from Tent map	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 1 0 1 1
		0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1
		1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1

	XOR operation	1111011011011000000001010000110110101011010010100011100111010 1011 0111000100001010011010010101100011001000111100110001100111011011
	Optimal 16 pixels	82 18 84 61 67 115 151 97 42 155 82 92 81 66 37 62

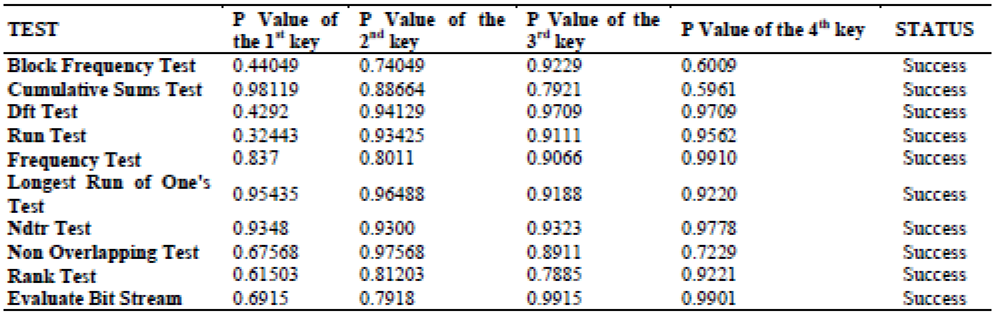
The 3rd retina image	Random bits generated from Tent map	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 1 0 1 1
		0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1
		1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1

	XOR operation	1100011101110110110100101001101011001001111010000000110010101001 1111000000001011011011010101100100101010011010011000110111001101 1
	Optimal 16 pixels	74 71 51 114 84 97 59 24 13 72 128 9 59 100 46 63

The 4th retina image	Random bits generated from Tent map	1 1 0 1 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 0 1 1 0 1 1 1 1 1 1 1 1 0 1 1
		0 0 0 1 1 1 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 1 0 0 1 1 1 1 0 0 1 1 0 0 0 1
		1 1 1 1 1 0 0 1 1 1 1 0 1 1 1 1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1

	XOR operation	1011111010100101110011100111010010010011011111001001111110100011 0011110101100110111110010011111000100101101010110001100111111011

Figure 8 Cryptographic keys for the sample retina images



TEST	P Value of the 1st key	P Value of the 2nd key	P Value of the 3rd key	P Value of the 4th key	STATUS
Block Frequency Test	0.44049	0.74049	0.9229	0.6009	Success
Cumulative Sums Test	0.98119	0.88664	0.7921	0.5961	Success
Dft Test	0.4292	0.94129	0.9709	0.9709	Success
Run Test	0.32443	0.93425	0.9111	0.9562	Success
Frequency Test	0.837	0.8011	0.9066	0.9910	Success
Longest Run of One's Test	0.95435	0.96488	0.9188	0.9220	Success
Ndtr Test	0.9348	0.9300	0.9323	0.9778	Success
Non Overlapping Test	0.67568	0.97568	0.8911	0.7229	Success
Rank Test	0.61503	0.81203	0.7885	0.9221	Success
Evaluate Bit Stream	0.6915	0.7918	0.9915	0.9901	Success

Figure 9 NIST analysis for generated keys

The proposed methodology demonstrated how to extract strong keys from best characteristics in the biometric retina by applying MPA, and using a chaotic map to give best-quality with random, unexpected, and non-producable keys. The acquired findings also demonstrated the effectiveness of the proposed approach. Several researchers should rely on optimization strategies for extracting robust characteristics from biometrics in the domains of identification and key production using biometrics.

Conclusion:

This research proposes a mechanism for a retina-based key generation that is both efficient and effective. By focusing on the use of MPA to pull out the best features from the the majority significant position of HWT of the retinal diagram, this suggested method provides a resilient, unpredictable, and unique random key. These extracted best features are used along chaotic maps to provide volatile arbitrary keys for cryptographic applications. The proposed method bypass all NIST standards and has a strong randomness attribute, according to experimental results on the used dataset. In future development, the produced key will be utilized to encrypt data using one of the asymmetric cryptography algorithms.

References:

1. Zhu H, Zhao C, Zhang X, Yang L. A novel iris and chaos-based random number generator. Comp and Sec. 2013 July;36:40–48.
2. Wei W, Jun Z. Image encryption algorithm Based on the key extracted from iris characteristics. In2013 IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI) 2013 Nov 19 (pp. 169-172). IEEE.
3. Bajwa G, Dantu R. Neurokey: Towards a new paradigm of cancelable biometrics-based key generation using electroencephalograms. Comp and Sec. 2016 Sep;62:95–113.
4. Nguyen D, Tran D, Ma W, Sharma D. Random Number Generators Based on EEG Non-linear and Chaotic Characteristics. J of Cyber Sec and Mobil. 2017 July;6(3):305–338.

5. Panchal G, Samanta D. A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security. Comp & Elec Eng. 2018 July;69:461–478.
6. Taha MA, Hasan TM, Sahib NM. Retina Random Number Generator for Security Applications. 2019 2nd Int Conference on Engineering Technology and its Applications (IICETA). 2019 Aug 27-28; Al-Najef, Iraq. 2019;99-104.
7. Faramarzi, A., et al., Marine Predators Algorithm: A Nature-inspired Metaheuristic. Expert Systems with Applications, 2020
8. Bansal M, Kardam H, Khairwal H, sharma J, Narang S. Review On Using Biometric Signals in Random Number Generators. Int J of Adv Res. 2019 April;7(4):1543–1550.
9. Mazhar AN, Naser EF. Hiding the Type of Skin Texture in Mice based on Fuzzy Clustering Technique. Baghdad Sci J. 2020 Sep;17(3):967–972.
10. Kaya T. Memristor and Trivium-based true random number generator. Physica A: Statistical Mechanics and its Applications. 2020 March;542:124071.
11. Pooja S, Arjun CV, Chethan S. Symmetric key generation with multimodal biometrics: A survey. In2016 International Conference on Circuits, Controls, Communi and Comp (I4C) 2016 Oct 4 (pp. 1-5). IEEE.
12. Fatima J, Syed AM, Akram MU. Feature point validation for improved retina recognition. In2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications 2013 Sep 9 (pp. 13-16). IEEE.
13. Waleed J, Jun HD, Abbas T, Hameed S, Hatem H. A Survey of Digital Image Watermarking Optimization based on Nature Inspired Algorithms NIAs. Int J of Sec and Its Applications. 2014;8(6):315–334.
14. Hao YY, Zhang GL, Xiong B. An Improved Glowworm Swarm Optimization Algorithm. In2018 International Conference on Machine Learning and Cybernetics (ICMLC) 2018 Jul 15 (Vol. 1, pp. 155-160). IEEE.
15. Krishnanand KN, Ghose D. Glowworm Swarm Optimization: Theory, Algorithms, and Applications. Studies in Comp Intelligence. 1st ed. Springer Int Publishing; 2017. 698.
16. Krishnanand KN, Ghose D. Detection of multiple source locations using a glowworm metaphor with applications to collective robotics. Proceedings 2005 IEEE Swarm Intelligence Symposium. 2005 June 8-10; Pasadena, CA, USA. 2005; 84-91.